6750-01-P]

FEDERAL TRADE COMMISSION

[File No. 192 3167]

Zoom Video Communications, Inc.; Analysis to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed consent agreement; request for comment.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis to Aid Public Comment describes both the allegations in the complaint and the terms of the consent order—embodied in the consent agreement—that would settle these allegations.

DATES: Comments must be received on or before **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Interested parties may file comments online or on paper by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Please write "Zoom Video Communications, Inc.; File No. 192 3167" on your comment, and file your comment online at *https://www.regulations.gov* by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Linda Holleran Kopp (202-326-2267), Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained from the FTC Website at this web address: https://www.ftc.gov/news-events/commission-actions.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]**. Write "Zoom Video Communications, Inc.; File No. 192 3167" on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the *https://www.regulations.gov* website.

Due to the public health emergency in response to the COVID-19 outbreak and the agency's heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comments online through the *https://www.regulations.gov* website.

If you prefer to file your comment on paper, write "Zoom Video Communications, Inc.; File No. 192 3167" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580; or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610

(Annex D), Washington, DC 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible website at *https://www.regulations.gov*, you are solely responsible for making sure your comment does not include any sensitive or confidential information. In particular, your comment should not include sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure your comment does not include sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential"—as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)—including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the *https://www.regulations.gov* website—as legally required by FTC Rule 4.9(b)—we cannot redact or remove your comment from that

website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at http://www.ftc.gov to read this Notice and the news release describing the proposed settlement. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*]**. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see https://www.ftc.gov/site-information/privacy-policy.

Analysis of Proposed Consent Order to Aid Public Comment

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from Zoom Video Communications, Inc. ("Zoom").

The proposed consent order ("proposed order") has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

This matter involves Zoom, a videoconferencing platform provider that provides customers with videoconferencing services and various add-on services, such as cloud storage. Zoom's core product is the Zoom "Meeting," which is a platform for one-on-one and group videoconferences. Users can also, among other things, chat with others in Meetings, share their screens, and record videoconferences.

In its proposed five-count complaint, the Commission alleges that Zoom violated Section 5(a) of the Federal Trade Commission Act. First, the proposed complaint alleges that Zoom misrepresented to users since at least June 2016 that they could secure all Meetings with end-to-end encryption. End-to-end encryption is a method of securing communications where an encrypted communication can only be deciphered by the communicating parties. No other person—not even the platform provider—can decrypt the communication because they do not possess the necessary cryptographic keys. Contrary to its representations to users, Zoom did not provide end-to-end encryption for all Meetings because Zoom's servers maintained the cryptographic keys that could allow Zoom to access the content of its customers' Meetings.

Second, the proposed complaint alleges that Zoom misrepresented the level of encryption it used to secure communications between participants using Zoom's video conferencing service. Specifically, Zoom had claimed since at least June 2016 that it secured Meetings, in part, with Advanced Encryption Standard (AES) and using a 256-bit encryption key ("AES 256-bit encryption"). The 256-bit encryption key refers to the length of the key needed to decrypt the communication. Generally speaking, longer encryption keys provides more confidentiality protection than shorter keys because there are more possible key combinations, thereby making it harder to find the correct key and crack the encryption. Contrary to its representation to users, Zoom in fact secured its Meetings with AES with a 128-bit encryption key.

Third, the proposed complaint alleges that Zoom misrepresented that, for users who opted to store recordings of their Zoom Meetings in Zoom's secure cloud storage ("Cloud Recordings"), Zoom would process and store such recordings in Zoom's cloud "once the meeting has ended." Contrary to its representations to users, Zoom kept Cloud Recordings on Zoom's servers for up to 60 days, unencrypted, before transferring them to Zoom's secure cloud storage, where they are then stored encrypted.

Fourth, the proposed complaint alleges that Zoom violated Section 5 when it installed a local hosted web server (called "ZoomOpener") on 3.8 million users' Mac computers. In July 2018, Zoom updated its application for Mac desktop computers by secretly deploying a web server onto users' computers. The ZoomOpener web server was designed to circumvent a security and privacy safeguard in Apple's Safari browser. Apple had updated its Safari browser to help defend its users from malicious actors and popular malware by requiring interaction with a dialogue box when a website or link attempts to launch an outside App. As a result of the new browser safeguard, users who clicked on a link to join a Zoom Meeting would receive an additional prompt that read, "Do you want to allow this page to open 'zoom.us'?" If the user selected "Allow", the browser would connect the user to the Meeting, while clicking "Cancel" would end the interaction and prevent the Zoom application from launching. The ZoomOpener web server was designed to avoid this extra prompt. It also remained on users' computers even after users deleted the Zoom application, and would automatically reinstall the Zoom app—without any user interaction—if the user clicked on a link to join a Zoom Meeting or visited a website that had a Zoom Meeting embedded in it.

The proposed complaint alleges that it was an unfair act or practice for Zoom, without adequate notice or consent, to circumvent the Safari browser safeguard without implementing any measures to compensate for the circumvented privacy and security protections. The proposed complaint alleges that doing so caused or was likely to cause substantial injury to consumers, that consumers could not reasonably avoid themselves, and that was not outweighed by countervailing benefits to consumers or competition. Apple removed the ZoomOpener web server from users' computers through an automatic update in July 2019.

Finally, the proposed complaint alleges Zoom violated Section 5 when it represented that it was updating its Mac application to resolve minor bug fixes, but failed

to disclose, or failed to disclose adequately, the material information that the update would deploy the ZoomOpener web server, that the web server would circumvent a Safari browser privacy and security safeguard, or that the web server would remain on users' computers even after they had uninstalled Zoom's Mac application.

Part I of the proposed order prohibits Zoom from misrepresenting its privacy and security practices in the future. It prohibits, for example, misrepresentations about Zoom's collection, maintenance, use, deletion, or disclosure of Covered Information; the security features, or any feature that impacts a third-party security feature, included in any Meeting Service; or the extent to which Respondent otherwise maintains the privacy, security, confidentiality, or integrity of Covered Information. "Covered Information" means information from or about an individual.

Part II of the proposed order requires Zoom to establish, implement, and maintain a comprehensive information security program that protects the security, confidentiality, and integrity of Covered Information. Among other things, Zoom must implement specific security safeguards, such as a security review for all new software, a vulnerability management program for its internal networks, security training for its employees, inventorying personal information stored in its systems and implementing data deletion policies, and other specific security measures, such as proper network segmentation and remote access authentication.

Part III of the proposed order requires Zoom to obtain initial and biennial data security assessments for twenty years.

Part IV of the agreement requires Zoom to disclose all material facts to the assessor and prohibits Respondent from misrepresenting any fact material to the assessments required by Part III.

Part V requires Zoom to submit an annual certification from a senior corporate manager (or senior officer responsible for its information security program) that it has

implemented the requirements of the Order, and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Part VI requires Zoom to submit a report to the Commission of its discovery of any Covered Incident. A "Covered Incident" is when any federal, state, or local law or regulation requires Zoom to notify any federal, state, or local government entity that information collected or received by Zoom from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization. Video and audio content are specifically included as a type of personal information that would trigger notification.

Parts VII through X of the proposed order are reporting and compliance provisions. Part VII requires acknowledgement of the order and dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part VIII ensures notification to the FTC of changes in corporate status and mandates that the company submit an initial compliance report to the FTC. Part IX requires the company to create and retain certain documents relating to its compliance with the order. Part X mandates that the company make available to the FTC information or subsequent compliance reports, as requested.

Part XI states that the proposed order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify in any way the proposed order's terms.

By direction of the Commission, Commissioner Chopra and Commissioner Slaughter dissenting.

April J. Tabor,

Acting Secretary.

Majority Statement of Chairman Joseph J. Simons, Commissioner Noah Joshua Phillips, and Commissioner Christine S. Wilson

At a time when millions of Americans are using videoconferencing services on a daily basis, the settlement that the Commission announces today ensures that Zoom will prioritize consumers' privacy and security. The Commission's complaint alleges that Zoom made misrepresentations regarding the strength of its security features and implemented a software update that circumvented a browser security feature. The proposed order provides immediate and important relief to consumers, addressing this conduct. The order requires that Zoom establish and implement a comprehensive security program that includes detailed and specific security measures. These obligations include reviews of all new software for common security vulnerabilities; quarterly scans of its internal network and prompt remediation of critical or severe vulnerabilities; and prohibitions against privacy and security misrepresentations.[1] This order will enable the Commission to seek significant penalties for noncompliance. This settlement provides critical, and timely, relief.

We are confident that the proposed relief appropriately addresses the conduct alleged in the complaint and is an effective, efficient resolution of this investigation. Our dissenting colleagues suggest additional areas for relief that likely would require protracted litigation to obtain. Given the effective relief this settlement provides, we see no need for that. Hundreds of millions of people use Zoom on a daily basis, often for free or through month-to-month contracts. We feel it is important to put in place measures to protect those users' privacy and security now, rather than expend scarce staff resources

[1]Although the complaint does not allege privacy violations, the order includes targeted fencing in relief providing privacy protections to consumers. For example, it prohibits Zoom from misrepresenting its privacy practices, and requires Zoom to implement changes to its naming procedures for saving or storing recorded videoconference meetings, and to develop data deletion policies and procedures. These and other requirements serve to protect consumers' privacy as well as the security of their information and communications.

on speculative, potential relief that a Court would not likely grant, given the facts here.[2] Our goal is a safe and secure Zoom that can continue to provide essential services to enable Americans to conduct business, engage in learning, participate in religious services, and stay connected. We applaud the FTC Staff for their professional and expeditious work to achieve this settlement in the midst of the pandemic. This case reflects the Commission's ongoing commitment to work on behalf of consumers to respond to the panoply of new challenges presented by COVID-19.

[2] Our dissenting colleagues also argue that the settlement is insufficient because it does not require Zoom to notify consumers of its past misconduct. The conduct at issue was broadly publicized and we believe the Commission's press release and business and consumer education provide ample information for consumers to learn more.

Dissenting Statement of Commissioner Rohit Chopra

Summary

- When companies deploy deception, this harms customers and honest competitors, and it distorts the marketplace. This is particularly problematic when it comes to the digital economy.
- Zoom's alleged security failures warrant serious action. But the FTC's proposed settlement includes no help for affected parties, no money, and no other meaningful accountability.
- The FTC's status quo approach to privacy, security, and other data protection law violations is ineffective. However, Commissioners can take a series of concrete steps to change this.

Introduction

Sometimes a new product becomes inextricably linked to the brand that made it popular. Kleenex, Band-Aids, and Frisbees are examples where the company became synonymous with the product.[1] This is particularly true in the digital economy where products can improve the use and capability of technology to the point of transforming its role in everyday life. We use "Google" as a verb when referring to use of a search engine. We "Uber" when we need a ride across town. And now, we "Zoom" when referring to videoconferencing. If becoming a verb threatens a trademark, firms fight against it. If it means becoming the default product in a market, they fight for it. But, profiting through unlawful means must come with real consequences.

Zoom (NASDAQ: ZM) did not invent web-based video conferencing. Indeed, there are many other players in the market. But Zoom succeeded in becoming the "default" for many businesses, both large and small, capturing a significant market share

[1] Mark Abadi, *Taser, Xerox, Popsicle, and 31 more brands-turned-household names*, BUSINESS INSIDER (June 3, 2018), https://www.businessinsider.com/google-taser-xerox-brand-names-generic-words-2018-5.

despite a crowded field. However, the allegations in the FTC's complaint raise questions whether Zoom's success – and the tens of billions of dollars of wealth created for its shareholders and executives in a short period of time – was advanced through fair play.[2] In my view, the evidence suggests that deception helped to create this windfall.

With businesses, families, schools, and even governments using Zoom to share extremely sensitive information, the alleged security vulnerabilities of this video conferencing platform raise major concerns, including threats to our privacy[3] and national security.[4]

Today, the Federal Trade Commission has voted to propose a settlement with Zoom that follows an unfortunate FTC formula. The settlement provides no help for affected users. It does nothing for small businesses that relied on Zoom's data protection claims. And it does not require Zoom to pay a dime. The Commission must change course.

Deception Distorts Competition

When companies need to act quickly to exploit an opportunity, deploying deception to steal users or sales from competing players is tantalizing. When video conferencing became a necessity for many businesses and families, existing players saw a potential gold mine. Even though we can all technically use multiple videoconferencing platforms as participants, a videoconferencing provider's monetization will largely be driven by how many businesses adopt its offering as their enterprise videoconferencing solution.[5] FTC prohibitions on unfair or deceptive practices are supposed to temper the temptation to deceive customers.

---

[2] Richard Waters, *Zoom to cash in on pandemic success with apps and events*, FINANCIAL TIMES (Oct. 14, 2020), https://www.ft.com/content/f1731672-e965-48a1-9362-bab122fc9bf4.

[3] In her voting statement, Commissioner Rebecca Kelly Slaughter details some of the key intersections between privacy and security.

[4] Sonam Sheth, *Foreign intelligence operatives are reportedly using online platforms and video-conferencing apps like Zoom to spy on Americans*, BUSINESS INSIDER (Apr. 9, 2020), https://www.businessinsider.com/foreign-intelligence-agents-china-spying-on-americans-zoom-2020-4.

[5] Zoom Video Communications, Inc., Oct. 2019 Quarterly Report (Form 10-Q) (Dec. 9, 2019), https://www.sec.gov/ix?doc=/Archives/edgar/data/1585521/000158552119000059/zm-20191031.htm.

Before the pandemic, Zoom primarily focused on business customers. Small and large businesses alike were looking for ways to connect with clients and business partners through video conferencing. Zoom competed with Microsoft's Skype, Microsoft's Teams, Cisco's WebEx, BlueJeans, and many other products. Comparison guides point out the different strong points of each service – from encryption to price.[6] In the summer of 2019, Zoom had over 600,000 customers that paid fees to use Zoom's services.[7] These customers were overwhelmingly small businesses.[8]

Small businesses often don't have employees dedicated to information security or even to information technology more broadly. That's why they rely on representations made by those they purchase software and services from. Many businesses want to ensure that any software application they use, including any video conferencing solution, comes with meaningful security standards. Zoom had to respond to this critical customer need if it was going to compete. Once the pandemic shut down workplaces across the country, businesses needed to find a reliable solution that was also secure. Many chose Zoom.[9]

Zoom sold its customers on the idea that it was an easy-to-use service that took "security seriously." However, when examining the company's engineering and product decisions, a different reality emerges. For example, as the complaint alleges, Zoom installed a web server onto users' computers, without permission, as an end-run that would circumvent a browser security feature – all to avoid an extra dialogue box.[10] Zoom went further: even if you managed to uninstall Zoom, it would not remove the web server.[11] And that web server could secretly re-install Zoom, even without your

---

[6] Kari Paul, *Worried about Zoom's privacy problems? A guide to your video-conferencing options*, THE GUARDIAN (Apr. 9, 2020), https://www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives.

[7] Compl., *In the Matter of Zoom Video Communications, Inc.*, Comm'n File No. 1923167 (Nov. 9, 2020).

[8] *Id*.

[9] Matt Torman, *5 Reasons Why Zoom Will Benefit Your Small Business*, ZOOM (Jan. 24, 2020), https://blog.zoom.us/zoom-video-communications-small-business-benefits/.

[10] Compl., *supra* note 7.

[11] David Murphy, *Remove Zoom From Your Mac Right Now*, LIFEHACKER (July 9, 2020), https://lifehacker.com/remove-zoom-from-your-mac-right-now-1836209383.

permission.[12] This is not just troubling conduct – this is what some have called "malware-like" behavior.[13]

This fervent attention to detail – going to great lengths to avoid a single dialogue box – did not extend to the security features it touted in sales materials.[14] The FTC's complaint details a litany of serious security allegations, from not using what is "the commonly accepted definition" of end-to-end encryption to being a year or more behind in patching software in its commercial environment.[15]

Zoom's Windfall

Zoom has "cashed in" on the pandemic.[16] While Zoom doesn't publicly share its total number of users, the company has confirmed that it has nearly four times the number of customers with 10 or more employees than they had at this time a year ago.[17] Their stock value has soared.[18] Zoom's CEO, Eric Yuan, has increased his net worth by almost $16 billion *since March*, and is now one of the wealthiest individuals in America.[19]

Zoom can now use this new market penetration to increase monetization for users who currently do not pay any fees. With the pandemic-driven expansion, Zoom has announced that they're going to make a platform pivot and begin to offer an app

---

[12] *Id.*

[13] Jacob Kastrenakes, *Zoom saw a huge increase in subscribers — and revenue — thanks to the pandemic*, THE VERGE (June 2, 2020), https://www.theverge.com/2020/6/2/21277006/zoom-q1-2021-earnings-coronavirus-pandemic-work-from-home.

[14] Compl., s*upra* note 7.

[15] Michael Lee & Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing*, THE INTERCEPT (Mar. 31, 2020), https://theintercept.com/2020/03/31/zoom-meeting-encryption/; Compl., s*upra* note 7; Oded Gal, *The Facts Around Zoom and Encryption for Meetings/Webinars*, ZOOM (Apr. 1, 2020), https://blog.zoom.us/facts-around-zoom-encryption-for-meetings-webinars/.

[16] Richard Waters, *Zoom to cash in on pandemic success with apps and events*, FINANCIAL TIMES (Oct. 14, 2020), https://www.ft.com/content/f1731672-e965-48a1-9362-bab122fc9bf4.

[17] *Id*.

[18] *Id*.

[19] Taylor Nicole Rogers*, Meet Eric Yuan, the founder and CEO of Zoom, who has made over $12 billion since March and now ranks among the 400 richest people in America*, BUSINESS INSIDER (Sep. 9, 2020), https://www.businessinsider.com/meet-zoom-billionaire-eric-yuan-career-net-worth-life; Kerry A. Dolan et al., *The Forbes 400: The Definitive Ranking of the Wealthiest Americans in 2020*, FORBES (Sep. 8, 2020), https://www.forbes.com/profile/eric-yuan/?list=forbes-400&sh=474b78c761bf.

marketplace and a paid events platform.[20] Zoom disclosed to its investors how a shift to a "platform and sales model allow[s] us to turn a single non-paying user into a full enterprise deployment."[21]

Zoom stands ready to emerge as a tech titan. But we should all be questioning whether Zoom and other tech titans expanded their empires through deception.[22] Zoom could have taken the time to ensure that its security was up to the right standards. But, in my view, Zoom saw the opportunity for massive growth by quickly leaping into the consumer market, allowing it to rapidly emerge as the new way to virtually celebrate birthdays and weddings and further solidify itself into our lives. But had Zoom followed the law, it might all be different.

Status Quo Approach to Privacy and Security Settlements

In matters like these, investigations should seek to uncover how customers were baited by any deception, how a company gained from any misconduct, and the motivations for this behavior. This approach can help shape an effective remedy. While deciding to resolve a matter through a settlement, regulators and enforcers must seek to help victims, take away gains, and fix underlying business incentives.

Of course, all settlements involve tradeoffs, but like other FTC data protection settlements, the FTC's proposed settlement with Zoom accomplishes none of these objectives. This is particularly troubling given the nature of the alleged deception. Key features of the FTC's proposed settlement include:

No help. Small businesses that purchased Zoom services or signed long-term contracts based on false representations are not even addressed in the Commission's

---

[20] *Supra* note 16.

[21] Zoom Video Communications, Inc., Quarterly Report (Form S-1) (Dec. 21, 2018), https://www.sec.gov/Archives/edgar/data/1585521/000095012318012479/filename1.htm.

[22] Decision and Order, *In the Matter of Google Inc.*, Comm'n File No. 1023136 (Oct. 24, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf; Decision and Order, *In the Matter of Facebook, Inc.*, Comm'n File No. 0923184 (July 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

order. They will not have the ability to be released from any contracts, seek refunds, or get credit toward future service. Similarly, Zoom's law-abiding competitors and other consumers affected by the alleged misconduct will not get anything to address how they were harmed.

No notice. The targets of deception deserve the dignity of knowing that the product they were using did not use the security features that were advertised. Notice also provides information on whether or not users need to take any specific further actions to protect themselves or their place of business. This is especially critical in cases where individuals may not know if they are affected. In this matter, Zoom's technology was integrated into white label products that may not use Zoom's brand. Notice is also helpful when victims receive no restitution.

No money. In my view, the evidence is clear that Zoom obtained substantial benefits through its alleged conduct. However, the resolution includes no monetary relief at all, despite existing FTC authority to seek it in settlements when conduct is dishonest or fraudulent. If the FTC was concerned about its ability to seek adequate monetary relief, it could have partnered with state law enforcers, many of whom can seek civil penalties for this same conduct.

No fault. The Commission's order includes no findings of fact or liability. In other words, Zoom admits nothing and the Commission's investigation makes no significant conclusions. This will make it more difficult for affected parties to exercise any contractual rights or seek help through private actions.

Earlier this year, after a number of security concerns emerged, the Attorney General of New York quickly took action, and Zoom signed a voluntary compliance agreement, which requires certain third-party reports and compliance with additional

standards.[23] The FTC's proposed settlement terms add some requirements to what Zoom has already agreed to with New York, largely involving additional independent monitoring and paperwork submissions. It is not clear to me that these new obligations are actually changing the way Zoom does business. In fact, Zoom may already be retaining third parties to assist with compliance as part of its contractual obligations with its largest customers.

Recommendations to Restore Credibility

To protect the public and promote fair markets, the FTC must be a credible law enforcement agency, especially when it comes to large players in digital markets. Our recent law enforcement actions raise questions that warrant careful attention if we aspire to be an effective enforcer. Below are some of the tangible steps the Commission should pursue:

1. Strengthen orders to emphasize more help for individual consumers and small businesses, rather than more paperwork.

When consumers and small businesses are the targets of unlawful data protection practices, the FTC's status quo approach often involves requiring the company engaged in misconduct to follow the law in the future and submit periodic paperwork. In certain orders, the Commission requires the retention of a third-party assessor, which the company might already be doing.

The FTC should focus its efforts on ensuring resolutions lead to meaningful help and assistance to affected consumers and small businesses. For example, the Commission could seek requirements that defendants respond to formal complaints and inquiries. This assists consumers while also allowing the Commission to track emerging harms and how the company is remediating them.

---

[23] Press Release, N.Y. Att'y Gen., Attorney General James Secures New Protections, Security Safeguards for All Zoom Users (May 7, 2020), https://ag.ny.gov/press-release/2020/attorney-general-james-secures-new-protections-security-safeguards-all-zoom-users.

Another way to help affected consumers and businesses is to order releases from any long-term contractual arrangements. When customers are baited with deceptive claims, it would be appropriate to allow them to be released from any contract lock-in or otherwise amend contractual terms to make customers whole. This would also help honest competitors regain some of the market share improperly diverted by deceptive conduct.

The Commission should seek notices to affected parties, so that these individuals and businesses can determine whether they need to take any action and whether they want to continue to do business with a company that engaged in any wrongdoing.

2. Investigate firms comprehensively across the FTC's mission.

The FTC is a unique institution with legal authorities related to data protection, consumer protection, and competition, all under one roof, rather than divided up across multiple agencies. It is critical that the agency use its authority to deter unfair or deceptive conduct in conjunction with our authority to deter unfair methods of competition. The agency can do more to comprehensively use its authorities across its mission, particularly when unfair or deceptive practices can advance dominance in digital markets. When we do not, investigations may result in ineffective resolutions that fail to fix the underlying problems and may increase the likelihood of recidivism. The Commission may need to reorganize its offices and divisions to ensure investigations are comprehensive.

3. Diversify the FTC's investigative teams to increase technical rigor.

Engineers, designers, and other technical experts can offer major contributions to our investigative teams. Many of the cases previously pursued by the FTC were the result of press coverage from technical experts, especially security researchers. In fact, an

independent researcher working in his private capacity was one of the first to discover a serious vulnerability in Zoom's product.[24]

Many of our peer agencies around the world approach investigations with diverse, interdisciplinary teams. Unfortunately, the Commission has deprived our litigators and enforcement attorneys of this needed expertise. The Commission should restore the role of the Chief Technologist and make a concerted effort to increase the proportion of technologists and others with technical knowledge in our investigative teams. If these individuals play meaningful leadership roles in our investigations, the agency can be much more effective.

With these technical skills and leadership in place, the Commission could proactively review the dominant digital products and services rather than primarily following up on concerning media reports after sensitive information or access has been at risk.

4. Restate existing legal precedent into clear rules of the road and trigger monetary remedies for violations.

Markets benefit when there are simple, clear rules of the road. This allows honest businesses to know what is and is not permissible. This especially helps small businesses and startups. On the other hand, ambiguity helps large incumbents who can hire lawyers and lobbyists to sidestep their obligations. The FTC can promote fair markets by restating accepted legal precedent and past Commission experience through an agency rulemaking. These would create no new substantive obligations on market participants. But once restated and enforced, violations trigger significant monetary relief.

Under the FTC Act, the Commission has a number of authorities to seek monetary relief. While one of these authorities, Section 13(b), is under considerable scrutiny in the

[24] The independent research solicited readers for contributions to assist with his work and pay off his student loans. Jonathan Leitschuh, *Zoom Zero Day: 4+ Million Webcams & maybe an RCE? Just get them to visit your website!*, INFOSEC WRITE-UPS (July 8, 2019), https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5.

courts, the Commission can also seek money by restating existing legal precedent through a rulemaking. When the Commission has issued prior orders for past misconduct in the market or there is other information indicating a widespread pattern of unfair or deceptive conduct, Section 18 of the FTC Act authorizes the Commission to define what constitutes an unfair or deceptive practice by rule. Violations of these rules can trigger liability for redress, damages, penalties, and more.

Over the years, the Commission has finalized a substantial number of orders related to data protection, including privacy and data security. There have also been developments in case law in the courts. The Commission should consider restating this past precedent into a rule under Section 18 or other appropriate statutes to provide clear guidance and systematically deter unlawful data protection practices.[25]

5. Demonstrate greater willingness to pursue administrative and federal court litigation.

Congress intended for the FTC to serve as an expert agency that analyzes emerging business practices and determines whether they might be unfair or deceptive. Administrative litigation and final Commission orders can provide important guidance to the marketplace on the agency's analytical approach. It can also serve as the basis for triggering financial liability for other market actors, pursuant to the Commission's Penalty Offense Authority.[26]

Federal court litigation pursued by our staff has contributed to strong outcomes and important development of the law. For example, in 2012, the FTC took action against Wyndham Hotels, a major hospitality chain the Commission charged with employing unfair data practices. Wyndham Hotels waged an aggressive defense, challenging the

---

[25] Statement of Commissioner Rohit Chopra Regarding the Report to Congress on Protecting Older Consumers, Comm'n File No. P144400 (Oct. 19, 2020), https://www.ftc.gov/system/files/documents/public_statements/1581862/p144400choprastatementolderamericansrpt.pdf.

[26] *See* Rohit Chopra & Samuel A.A. Levine, *The Case for Resurrecting the FTC Act's Penalty Offense Authority* (Oct. 29, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721256.

FTC's theories before the District Court and the Third Circuit Court of Appeals. The court's ruling cemented the Commission's ability to target lax data security practices under existing law.

The public benefits from the work of the FTC's talented investigators and litigators across the agency, and as Commissioners, we should have confidence that they can hold accountable even the largest players in the economy. But recently, when it comes to data protection, FTC Commissioners have rarely voted to authorize agency staff to sue national players for misconduct. We must do more to safeguard against any perception about the agency's unwillingness to litigate.

6. Increase cooperation with international, federal, and state partners.

When it comes to data protection abuses and other harmful practices by large technology firms, these concerns are increasingly global. The FTC can use its resources more effectively and obtain superior outcomes when it cooperates with other law enforcement partners.

In the Ashley Madison matter, the FTC partnered with the Office of the Privacy Commissioner of Canada, Office of the Australian Information Commissioner, and many state attorneys general. This action was the result of significant cooperation and ultimately led to a joint resolution.[27] Unfortunately, this is too rare.

The FTC can rely on key provisions of the U.S. SAFE WEB Act that allow the FTC to share information with foreign counterparts to combat deceptive or unfair practices that cross national borders. Domestically, agencies can form multistate working groups to combine resources and leverage a diverse set of legal authorities.

In the matter before the Commission today, the conduct at issue might have also violated state laws. Additional liability triggered by these laws could have led to a

[27] Press Release, Fed. Trade Comm'n, Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information (Dec. 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting.

resolution with a far superior outcome. Instead, other law enforcement agencies both at home and abroad will likely need to continue to scrutinize Zoom's practices, given the FTC's proposed resolution.

In addition, the Commission needs to rethink its approach to enforcing privacy promises by large technology firms related to their participation in international agreements, such as the EU-U.S. Privacy Shield Framework. Zoom's conduct may have violated key aspects of the framework, and I believe the Commission should have taken action accordingly. The Commission should now fully cooperate with our international partners to ensure that they can proceed with appropriate sanctions.

7. Determine whether third-party assessments are effective.

A common provision in FTC orders requires the defendant to retain a third party to monitor compliance and the company's data protection protocols. However, it is unclear whether those assessments are truly effective when it comes to deterring or uncovering misconduct. For example, in the FTC's investigation of Facebook for compliance with its privacy obligations under a 2012 Commission order, the FTC alleged major violations of the order even though an independent third party, PriceWaterhouseCoopers (PwC), was supposedly watching over the company's compliance.[28]

Additionally, the Commission's decision to not proactively make certain information about these third party reports public limits our ability to determine their effectiveness.[29] If independent researchers and journalists – often the ones who originally discovered data protection failures in the first place – had access to these reports,

---

[28] *See* Nitasha Tiku, *Facebook's 2017 Privacy Audit Didn't Catch Cambridge Analytica*, WIRED (Apr. 19, 2018), https://www.wired.com/story/facebooks-2017-privacy-audit-didnt-catch-cambridge-analytica/; S*ee also* Dissenting Statement of Commissioner Rohit Chopra In re Facebook, Inc., Comm'n File No. 1823109 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

[29] Statement of Commissioner Rohit Chopra In the Matter of Uber Technologies, Inc., Comm'n File No. 1523054 (Oct. 26, 2018), https://www.ftc.gov/system/files/documents/public_statements/1418195/152_3054_c-4662_uber_technologies_chopra_statement.pdf.

companies and third-party monitors might take them more seriously, which would help to fulfill the intended purpose of their efforts.

Conclusion

This year families have said their final goodbyes to loved ones over Zoom.[30] Desperate parents have propped their children in front of screens for school and hoped that they won't fall too far behind.[31] Small businesses have been turned upside down by our new way of life and have fought for a chance at survival by switching to doing business virtually.[32] But when tech companies cheat, rather than compete, and then face no meaningful accountability, all of us suffer.

I am concerned that Zoom simply thought that the FTC's law enforcement inquiry wasn't serious. That's probably why the company didn't even bother to disclose the agency's inquiry to its investors.[33] The company seemed to guess that the FTC wouldn't do anything to materially impact their business. Sadly, for the public, they guessed right. Given the company's approach, efforts to hold Zoom accountable by regulators and enforcers in the U.S. and abroad will clearly need to continue.

Finally, the Federal Trade Commission has requested greater authority from Congress to protect Americans from abuse and misuse of personal data. But, actions like today's proposed settlement undermine these efforts. The agency must demonstrate that it is willing to use all of its existing tools to protect consumers and the market. Only then will the Commission be entrusted to take on more responsibilities.

---

[30] Sarah Zhang, *The Pandemic Broke End-of-Life Care*, THE ATLANTIC (June 16, 2020), https://www.theatlantic.com/health/archive/2020/06/palliative-care-covid-19-icu/613072/.

[31] Heather Kelly, *Kids used to love screen time. Then schools made Zoom mandatory all day long.*, WASH. POST (Sep. 4, 2020), https://www.washingtonpost.com/technology/2020/09/04/screentime-school-distance/.

[32] Justin Lahart, *Covid Is Crushing Small Businesses. That's Bad News for American Innovation.*, WALL STREET J. https://www.wsj.com/articles/covid-is-crushing-small-businesses-thats-bad-news-for-american-innovation-11602235804.

[33] Zoom Video Communications, Inc., July 2020 Quarterly Report (Form 10-Q) (Sep. 3, 2020), https://www.sec.gov/ix?doc=/Archives/edgar/data/1585521/000158552120000238/zm-20200731.htm. When publicly traded firms do not disclose to their investors that they are facing a federal law enforcement inquiry, this suggests that they do not believe the inquiry is material to their financial or operational performance.

It is critical that we restore the agency's credibility deficit when it comes to oversight of the digital economy. This does not stem from a lack of authority or resources or capabilities from our staff – it stems from the policy and enforcement approach of the Commission, and this needs to change.

For these reasons, I respectfully dissent.

Dissenting Statement of Commissioner Rebecca Kelly Slaughter

Most weekday mornings, my two elementary-age children log on to school through Zoom. Their faces, voices, and occasional silliness are all captured in the Zoom classroom. I try not to dwell on what might occasionally float through in the background of their camera or microphone, but, like many families, we've had moments in our home where we are very much live. After my older kids settle in for class, my own workday begins in earnest and typically involves a series of confidential discussions often made possible through a Zoom meeting. My experience is not unique: Zoom expanded from 10 million daily users last December to over 300 million daily participants this spring. Zoom's overnight expansion from a modest video conferencing company to a company providing critical infrastructure for business, government, education, and social connection raises important questions for the Commission's obligations to protect consumer security and privacy.

Years before the global pandemic would make Zoom a household name, the company made decisions that threatened the security and privacy of its longstanding core business customers. Yet the Commission's proposed settlement provides no recourse for these paying customers. When Zoom's user base rapidly expanded, its failure to prioritize privacy and security suddenly posed a much more serious risk in terms of scope and scale. This proposed settlement, however, requires Zoom only to establish procedures designed to protect user *security* and fails to impose any

requirements directly protecting user *privacy*. For a company offering services such as Zoom's, users must be able to trust that the company is committed to ensuring security and privacy alike.

Because the proposed resolution fails to require Zoom to address privacy as well as security, and because it fails to require Zoom to take any steps to correct the deception we charge it perpetrated on its paying clients, I respectfully dissent.[1]

Zoom's Practices

As set forth in the Commission's complaint, Zoom engaged in a series of practices that undermined the security and privacy of its users. First, we allege Zoom made multiple misrepresentations about its use of encryption. As charged in the complaint, Zoom made false statements about its encryption being "end-to-end," the level of encryption that it offered, and the time it took to store recorded meetings in an encrypted server.[1]

Zoom's problematic conduct was not limited to deception. The complaint charges that beginning in July 2018, Zoom secretly *and unfairly* deployed a web server, called the "ZoomOpener," to circumvent certain Apple privacy and security safeguards enjoyed by Safari browser users. Because of these safeguards, Safari users who clicked on a link to join a Zoom meeting would receive an additional prompt that read, "Do you want to allow this page to open 'zoom.us'?"[2] That is until, we allege, Zoom overrode this feature through its secret ZoomOpener, which bypassed the Safari safeguard to directly launch the Zoom App.[3] The user was then automatically placed in the Zoom meeting, and, if the user had not changed her

---

[1] *See* Complaint ¶¶ 16–33.

[2] Complaint ¶ 35. If the user selected "Allow," the browser would connect the user to the Zoom meeting. *Id*. This safeguard was not specific to Zoom; Apple had designed its Safari browser to help defend its users from malicious actors and popular malware by requiring interaction with a dialogue box whenever any website or link attempted to launch an outside app. *Id*. at ¶ 34.

[3] *Id*. at ¶ 36.

default video settings, her webcam was activated.[4]

In addition to these unfair and deceptive practices, which the Commission charged as law violations, there has been extensive public reporting on several other Zoom practices that raised serious privacy concerns. For example, Zoom business customers who subscribed to a service called "LinkedIn Sales Navigator" had access to LinkedIn profile data about other users in a meeting—even when the other user wished to remain anonymous.[5] Additionally, Security researchers found that Zoom-meeting video recordings saved on Zoom's cloud servers had a predictable URL structure and were thus easy to find and view.[6] And of course there was widespread coverage of "Zoom-bombing," in which uninvited users crashed Zoom meetings.[7] Zoom took steps to address these vulnerabilities after they surfaced by changing naming conventions, permanently removing the LinkedIn Sales Navigator app,[8] and requiring meeting passwords as the default setting for more Zoom users,[9] but these problems suggest Zoom's approach to user privacy was fundamentally reactive rather than proactive.

Lack of Privacy Protections

Too often we treat data security and privacy as distinct concerns that can be separately preserved. In reality, protecting a consumer's privacy and providing strong data security are closely intertwined, and when we solve only for one we fail to secure

---

[4] *Id*. at ¶ 37.

[5] *See* Aaron Krolik and Natasha Singer, *A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles*, N.Y. Times (Apr. 2, 2020), https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html. Zoom subsequently stated that it had disabled the feature.

[6] *See* Paul Wagenseil, *Zoom security issues: Here's everything that's gone wrong (so far)*, Tom's Guide (Nov. 3, 2020), https://www.tomsguide.com/news/zoom-security-privacy-woes.

[7] *See* Jay Peters, *Zoom adds new security and privacy measures to prevent Zoombombing*, The Verge (Apr. 3, 2020), https://www.theverge.com/2020/4/3/21207643/zoom-security-privacy-zoombombing-passwords-waiting-rooms- default.

[8] *See* Eric S. Yuan, *A Message To Our Users*, Zoom Blog (Apr. 1, 2020), https://blog.zoom.us/a-message-to-our- users/.

[9] *See* Deepthi Jayarajan, *Enhanced Password Capabilities for Zoom Meetings, Webinars & Cloud Recordings*, Zoom Blog (Apr. 14, 2020), https://blog.zoom.us/enhanced-password-capabilities-for-zoom-meetings-webinars-cloud- recordings/.

either. The Commission's proposed order resolving its allegations against Zoom requires the company to establish an information-security program and submit to related independent third-party assessments. These provisions strive to improve data-security practices at the company and to send a signal to others regarding the baseline for adequate data-security considerations. Nowhere, however, is consumer privacy even mentioned in these provisions. This omission reflects a failure by the majority to understand that the reason customers care about security measures in products like Zoom is that they value their privacy.

Some might argue that sound data security practices should naturally guarantee consumer privacy. I disagree. Strong security is necessary for consumer privacy, but it does not guarantee its achievement. Zoom's launch of its "ZoomOpener" to undermine the Apple Safari browser protections is an instructive example. Zoom prioritized maintaining its one-click functionality for users over privacy and security protections offered by Apple. The Commission's proposed order tries to solve for this problem solely as a security issue and makes it difficult for Zoom to bypass third-party security features in the future. But the order does not address the core problem: Zoom's demonstrated inclination to prioritize some features, particularly ease of use, over privacy protections. Dumping Safari users automatically into a Zoom meeting, with their camera on, the first time they clicked on a link was not only a data-security failing—it was a privacy failing.

Similarly, we often discuss data encryption as a security issue, which of course it is, but we should simultaneously be recognizing it as a privacy issue. When customers choose encrypted communications, it is because they value their privacy in the content of their conversations. Treating encryption failures as a security-only issue fails to recognize the important privacy implications.

The FTC has approached privacy and security issues with related but distinct remedies: by imposing a comprehensive privacy program (as we did in *FTC v. Uber*) or by imposing a comprehensive information security program (as we did in *FTC v. Equifax*). This case provides a perfect example of a place where we ought to have required elements of both privacy and security programs. A more effective order would require Zoom to engage in a review of the risks to consumer *privacy* presented by its products and services, to implement procedures to routinely review such risks, and to build in privacy-risk mitigation before implementing any new or modified product, service, or practice. The Commission required this type of privacy-focused inquiry in the "Privacy Review Statement" provisions of its order in the *FTC v. Facebook* matter.[10] Privacy-focused provisions such as these should either be added to relevant data- privacy orders as a separate privacy program or review, or the Commission's information security programs should be modified to better integrate privacy and security.

When companies offer services with serious security and privacy implications for their users, the Commission must make sure that its orders address not only security but also privacy.

No Recourse for Customers

As of July 2019, Zoom had approximately 600,000 paying customers, and approximately 88% of those customers were small businesses with ten or fewer employees.[11] In securing these customers, the Commission charges that Zoom made express representations regarding its encryption offerings that were false. Yet, the proposed order does not require Zoom to take any steps to mitigate the impact of these statements we contend are false. Zoom is not required to offer redress, refunds, or even

---

[10] To be clear, I am not suggesting that Zoom's conduct giving rise to this matter and Facebook's order violations are equivalents. Nor do the companies share similar business models. But in terms of the importance of consumer privacy, hundreds of millions of users are entrusting Zoom with some of their most sensitive interactions, and they are doing so from their homes.

[11] Complaint ¶ 9.

notice to its customers that material claims regarding the security of its services were false. This failure of the proposed settlement does a disservice to Zoom's customers, and substantially limits the deterrence value of the case.

Finally, I join Commissioner Chopra's call for the Commission to engage in critical reflection to strengthen our enforcement efforts regarding technology across the board—from investigation to resolution.[12]

[FR Doc. 2020-25130 Filed: 11/12/2020 8:45 am; Publication Date: 11/13/2020]

[12] Commissioner Chopra's dissenting statement sets forth an excellent list of *Recommendations and Corrective Actions* for the Commission to consider to improve the effectiveness of our enforcement efforts.